数理解析研究所講究録
第378巻 1980年 76-81

2次体の類数が1であることの判定法について

岐阜高専　　久綱　正和

§0. G. Rabinowitsch [3] はユークリッドの互除法を拡張し，虚2次体 $\mathbb{Q}(\sqrt{D})$, $D=1-4m<0$, の類数が1であるか否かを判定する，次の定理を得た：

定理　虚2次体 $\mathbb{Q}(\sqrt{D})$, $D=1-4m<0$, の類数が1であるための必要十分条件は，$1\leq x\leq m-1$ なるすべての整数 x に対して，x^2-x+m が素数となることである。

Rabinowitsch は実2次体については何も言っていないが，彼の方法は実2次体に対しても有効であり，虚2次体と類似の判定法が得られる：

定理　実2次体 $\mathbb{Q}(\sqrt{D})$, $D=1+4m>0$, において，$1\leq x\leq\sqrt{m}-1$ なるすべての整数 x に対して，$-x^2+x+m$ が素数

であるならば，その類数は1である。

例　$\mathbb{Q}(\sqrt{437})$，$437 = 1 + 4 \cdot 109$，$9 < \sqrt{109} - 1 < 10$.

$1 \leq x \leq 9$ のとき，$-x^2 + x + m = 109, 107, 103, 97, 89, 79, 67, 53$

37 はすべて素数であり，従って類数は1である。

§1. まず，一般の代数体 K において考える。K の整数環を $\mathfrak{o}_K$ で表わす。$\alpha \in K$ のノルムを $N\alpha$ で表わす.

定理1　K の類数が1であるための必要十分条件は，α/β, $\beta/\alpha \notin \mathfrak{o}_K$ なる任意の $\alpha, \beta \in \mathfrak{o}_K$ に対して，次の不等式を満たす $\xi, \eta \in \mathfrak{o}_K$ が存在することである：

$$0 < |N(\alpha\xi - \beta\eta)| < |N\beta|$$

証明はRabinowitschの方法と同じである。定理1の不等式を満たさない α, β に注目して，次の用語を定義する。

定義　K の数 $\alpha/\beta \notin \mathfrak{o}_K$ が störend であるとは，すべての $\xi, \eta \in \mathfrak{o}_K$ に対して

$$|N(\alpha/\beta \cdot \xi - \eta)| \geqq 1$$

が成立することである。

この用語を用いると，定理1は次のように言い換えられる：

定理1′　Kの類数が1であるための必要十分条件は，Kの中に störend 分数が存在しないことである。

störend 分数には次の性質がある。

1. α/β が störend ならば，任意の $\xi \in \mathfrak{o}_K$ に対して，$\alpha/\beta + \xi$，$\alpha/\beta \cdot \xi \ (\notin \mathfrak{o}_K)$ も störend である。
2. 有理分数 $a/b \ (\notin \mathbb{Z})$ は störend ではない。

§2．ここでは実2次体 $K = \mathbb{Q}(\sqrt{D})$，$D > 0$，について調べる。

$$\vartheta = \begin{cases} (1+\sqrt{D})/2, & D \equiv 1 \pmod 4 \\ \sqrt{D}, & D \equiv 2, 3 \pmod 4 \end{cases}$$

とすれば，$1, \vartheta$ は $\mathfrak{o}_K$ の基底になる。

命題1　Kの類数が1より大きいならば，次の形の störend 分数が存在する：

$$\frac{a-\vartheta}{p} \quad ; \quad p = \text{素数} \leqq \begin{cases} \sqrt{m}, & D = 1+4m \\ \sqrt{D}, & D \equiv 2, 3 \pmod 4 \end{cases}, \quad 0 \leqq a < p$$

命題2　$N(a-\vartheta)$ が p と互に素であるか，あるいは

$|N(a+kp-\vartheta)| < p^2$ を満たす有理整数 k が存在すれば，$(a-\vartheta)/p$ は störend ではない．

命題 3. $(a-\vartheta)/p$ が störend であるならば，$\left(\frac{D}{p}\right) \neq -1$.

命題 1, 2, 3 より次の判定法を得る．

定理 2. $1 < p \leq \begin{cases} \sqrt{m}, & D = 1+4m \\ \sqrt{D}, & D \equiv 2, 3 \pmod 4 \end{cases}$ なる任意の有理素数と，$0 \leq a < p$ なる有理整数 a に対して，$N(a-\vartheta)$ が p と互に素であるかあるいは $|N(a+kp-\vartheta)| < p^2$ を満たす有理整数 k が存在すれば，実 2 次体 $\mathbb{Q}(\sqrt{D})$ の類数は 1 である．

系 1. $D = 1+4m$, m = 奇数 とする．$2 < p \leq \sqrt{m}$ なるすべての有理素数 p に対して $\left(\frac{D}{p}\right) = -1$ ならば，実 2 次体 $\mathbb{Q}(\sqrt{D})$ の類数は 1 である．

系 2. $D = 1+4m$, p は $\leq \sqrt{m}$ なる最大の有理素数とする．$1 \leq x \leq p-1$ なるすべての有理整数 x に対して，$-N(x-\vartheta) = -x^2+x+m$ が有理素数ならば，実 2 次体 $\mathbb{Q}(\sqrt{D})$ の類数は 1 である．

[注]　$1 < D < 2{,}000$ の範囲で，系 1，2 の条件を満たす D は次の 9 個である：

$$D = 5,\ 13,\ 21,\ 29,\ 53,\ 77,\ 173,\ 293,\ 437\ .$$

実 2 次体を，その判別式が唯一の奇素数を含む場合に限定すると，より有効な判定法が得られる。

補題 (1)　$D = 1+4m$ の場合

任意の素数 p と，$0 \le a \le (p-1)/2$ なる任意の有理整数 a に対して，

$$(a-\vartheta)/p \ : \text{störend} \iff (p+1-a-\vartheta)/p \ : \text{störend}$$

(2)　$D \equiv 2, 3 \pmod 4$ の場合

任意の素数 p と，$1 \le a \le (p-1)/2$ なる任意の有理整数 a に対して，

$$(a-\vartheta)/p \ : \text{störend} \iff (p-a-\vartheta)/p \ : \text{störend}$$

命題 4　(1)　$D = 1+4m =$ 素数 の場合

$1 < p \le \sqrt{m}$ なる任意の素数 p に対して，$(a-\vartheta)/p$，$0 \le a < p$ は高々 1 つを除いて störend でないならば，実 2 次体 $\mathbb{Q}(\sqrt{D})$ の類数は 1 である。

(2)　$D = q,\ 2q$ ；$q =$ 素数 $\equiv 3 \pmod 4$ の場合

$2 < p < \sqrt{D}$ なる任意の素数 p に対して，$(a-\vartheta)/p$，$0 \leq a < p$ は高々1つを除いて störend でないならば，実2次体 $\mathbb{Q}(\sqrt{D})$ の類数は1である。

定理2と命題4を用いると，実2次体 $\mathbb{Q}(\sqrt{D})$ の類数が1であるか否かの判定が割合できる。特に，D の値が小さいときは有効である。

例　$D = 161 = 1 + 4 \cdot 40$．$1 < p \leq \sqrt{40}$ なる素数は 2，3，5．

x	1	2	3	4	5	6	7
$-N(x-\vartheta)$	40	38	34	28	20	10	−2

より $\mathbb{Q}(\sqrt{161})$ の類数は1であることが分かる．

参考文献

[1] Kutsuna, M. : On a criterion for the class number of a quadratic number field to be one , to appear in Nagoya Math. J.

[2] Nagel, T. : Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. U. Hamburg 1 (1922), 140-150

[3] Rabinowitsch, G. : Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern, J. reine angew. Math. 142 (1913), 153-164.